EETIMES

Consumer success: it comes down to innovation

By Fred von Lohmann, Senior Intellectual Property Attorney, Electronic Frontier Foundation, San Francisco, Calif., EE Times
April 18, 2003 (1:17 p.m. EST)
URL: http://www.eetimes.com/story/OEG20030418S0034

The entertainment industries are on a crusade to add "content protection" technologies to all sorts of digital products. Yet the "protection" technologies are often so ineffectual as to be virtually useless at securing content.

A lot of engineers are wondering just what's going on here? In their efforts to impose technologies to protect "content," why are the entertainment industries drawn to weak protection technologies?

But, maybe it's not about "protecting content" at all, but rather controlling innovation. In calling for pervasive "digital rights management," or DRM, technologies, entertainment industry lobbyists generally point to a need to solve the problem of "Internet piracy" as exemplified by the peer-to-peer descendants of Napster.

If stopping file-sharing is the goal, however, the task is a hard one. So long as individuals continue to have access to networks and technologies that enable easy copying and transmission of digital bits, all it takes is one person to defeat a DRM technology, extract the content, and inject it into the network.

From there, the cat will be out of the bag — the DRM, having been stripped away, is no longer even a "speed bump" to even the unsophisticated user. With this threat model in mind, you'd think that entertainment companies would be responding with highly robust DRM technologies.

For example, Hollywood is currently pressing the Federal Communications Commission (FCC) to adopt a protection regime for digital television built on a "broadcast flag." In its proposal, the precious television programming is broadcast in-the-clear, in an open standard (an 8/VSB-modulated MPEG-2 transport stream, described in ATSC A/53B) that has been independently implemented by several parties since it was standardized over seven years ago.

Rather than protecting the content, the plan is to have the FCC regulate any device that can modulate or demodulate a DTV signal, requiring it to include mandatory DRM technologies that will lock up demodulated MPEG files. This is a bit like projecting a movie on the side of city hall, then protecting it by demanding that passers-by avert their eyes.

There are plenty of other examples of fatally flawed DRM systems in the field, including copy-protection technology for audio CDs that was recently defeated with a felt tip marker. The most widely deployed failure, however, is the content protection used on DVDs.

Prior to the introduction of the DVD format, major motion picture studios offered many of the same arguments that they offer today with respect to DRM technologies like the broadcast flag. The movie studios argued that digital video formats created entirely new and

unique risks to their businesses-people would be able to duplicate and distribute their movies without permission. They said that these risks were so grave that they weren't willing to release their movies on DVD without some protection.

In response to this argument, an encryption-based content protection system known as the Content Scramble System (CSS) was developed and integrated into what became the DVD format.

Today, vendors who want to build devices capable of playing CSS-protected DVDs must enter into licensing agreements that impose strict limits on the kinds of capabilities that may be included in DVD devices.

While offering more protection than an unencrypted system like the broadcast flag, CSS was hopelessly flawed. First, it depended on global shared secrets that, once compromised, would unlock all DVDs on all players. Second, the encryption relied on 40-bit keys, which were vulnerable to brute force attacks. Serious implementation errors further undermined the security offered by CSS.

Not surprisingly, CSS was defeated by hobbyists soon after attaining mainstream acceptance, most famously by a loose-knit group that included a Norwegian teenager named Jon Johansen.

Despite legal efforts to ban the distribution of DVD decryption tools, those tools continue to be widely available today from both from retail and Internet sources. Once decrypted, a DVD movie can be played on any PC. As a result, DVD content is widely available today from unauthorized sources.

Bandwidth limits

The only meaningful constraint on this activity arises not from the content protection offered by CSS or the licensing obligations imposed by the CSS licensing entities, but rather from the limitations imposed by the limited bandwidth available to the American broadband subscriber.

In short, the DVD experience illustrates the total obsolescence of the "speed bump" model of content protection in a networked environment. If all it takes is one leak to free the content, then leaky DRM won't stop "Internet piracy." In fact, as four Microsoft researchers recently concluded in an influential paper entitled "The Darknet and the Future of Content Distribution," weak DRM systems are actually counter-productive, as they create incentives for otherwise law-abiding individuals to seek out unauthorized channels when they find their desires frustrated by DRM systems.

Notwithstanding the failure of CSS as a protection technology, DVDs are selling in record numbers. It seems that "content protection" was not necessary to support the market for DVDs. Hollywood was wrong.

But the imposition of CSS on the DVD format has left a distinct legacy-not in slowing unauthorized Internet redistribution, but in impediments to innovation. While CSS presents no "speed bump" to those intent on downloading movies from the Internet, the burdens imposed by CSS licensing requirements means that innovative engineers can only create those new products that the conservative, technophobic movie studios approve of in advance.

For example, CSS license terms have made it fantastically hard to get a DVD player with a

digital video output, requiring innovators to inject superfluous digital-to-analog-to-digital conversions in order to interface DVD players with new digital display devices. Similarly, innovators eager to deliver in-home "entertainment servers" capable of streaming digital video to multiple televisions or PCs over home networks cannot legally build tools to copy DVDs onto server hard drives.

Before new features can be added to DVD players, innovators must persuade the CSS licensing entities to permit them. The governance structure of these entities requires consensus among the motion picture, consumer electronics, and information technology industries, so no one industry can force a specification or rule change on the other industries.

Consequently, DVD innovators who need adjustments to existing DVD standards must first convince their "industry" (i.e., their competitors) of the wisdom of a new DVD product category, then must convince two other "industries" (which may include further competitors), and only then will be allowed to ship their product.

Put another way, thanks to CSS, today the entertainment industries have a veto right over innovation in the DVD market. That enduring advantage, bestowed by CSS on the entertainment industries at the expense of technology innovators, will continue whether or not CSS is actually effective at stopping "Internet piracy."

The same is true for the "broadcast flag" and other content protection mandates being pushed by the entertainment industries. Whether they are effective as an engineering matter may be much less important than whether they effectively give Hollywood a brake lever on innovations that disrupt their existing business arrangements.

Fred von Lohmann will a participate on the panel on Key Challenges for Consumer Media Products at the Embedded Systems Conference.